INSTITUTO FEDERAL GOIANO – CAMPUS CERES
BACHARELADO EM SISTEMA DE INFORMAÇÃO
JOSÉ PEDRO ALVES NETO

SEGURANÇA E VULNERABILIDADES EM REDES WI-FI E MÓVEIS: RISCOS E PROTEÇÃO DE DADOS EM TRANSAÇÕES BANCÁRIAS

CERES-GO, 2025

INSTITUTO FEDERAL
Goiano
Campus Trindade

JOSÉ PEDRO ALVES NETO

SEGURANÇA E VULNERABILIDADES EM REDES WI-FI E MÓVEIS: RISCOS E PROTEÇÃO DE DADOS EM TRANSAÇÕES BANCÁRIAS

Trabalho de Conclusão de Curso de Graduação em Sistema da Informação, orientado pelo Prof. Dr. Roitier Campos Gonçalves, aprovado em _.

CERES-GO, 2025

REVISTA CONTEMPORÂNEA

e-ISSN 2447-0961

Qualis CAPES 2017-2020: B1

DECLARAÇÃO

Revista Contemporânea, ISSN 2447-0961, declara para os devidos fins, que o artigo intitulado SEGURANÇA E VULNERABILIDADES EM REDES WI-FI E MÓVEIS: RISCOS E PROTEÇÃO DE DADOS EM TRANSAÇÕES BANCÁRIAS de autoria de José Pedro Alves Neto, foi publicado no v.5, n.5, de 2025.

A revista é on-line, e os artigos podem ser encontrados ao acessar o link:

https://ojs.revistacontemporanea.com/ojs/index.php/home/issue/view/40

DOI: https://doi.org/10.56083/RCV5N5-126

Por ser a expressão da verdade, firmamos a presente declaração.

Curitiba, 29 maio 2025.

Equipe Edito

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO

PARA DISPONIBILIZAR PRODUÇÕES TÉCNICO-CIENTÍFICAS NO REPOSITÓRIO INSTITUCIONAL DO IF GOIANO

Com base no disposto na Lei Federal nº 9.610, de 19 de fevereiro de 1998, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia Goiano a disponibilizar gratuitamente o documento em formato digital no Repositório Institucional do IF Goiano (RIIF Goiano), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IF Goiano.

IDENTIFICAÇÃO DA PRODUÇÃO TÉCNICO-CIENTÍFICA

- ☐ Tese (doutorado)
- ☐ Dissertação (mestrado)
- ☐ Monografia (especialização)
- ☑ TCC (graduação)
- ☐ Artigo científico
- ☐ Capítulo de livro
- ☐ Livro
- ☐ Trabalho apresentado em evento
- ☐ Produto técnico e educacional - Tipo:

Nome completo do autor:
JOSÉ PEDRO ALVES NETO

Matrícula:
2019103202030377

Título do trabalho:
SEGURANÇA E VULNERABILIDADES EM REDES WI-FI E MÓVEIS: RISCOS E PROTEÇÃO DE DADOS EM TRANSAÇÕES BANCÁRIAS

RESTRIÇÕES DE ACESSO AO DOCUMENTO

Documento confidencial: ☐ Não ☐ Sim, justifique:

Informe a data que poderá ser disponibilizado no RIIF Goiano: ☐/☐/☐

O documento está sujeito a registro de patente? ☐ Sim ☐ Não

O documento pode vir a ser publicado como livro? ☐ Sim ☐ Não

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O(a) referido(a) autor(a) declara:

• Que o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;

• Que obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autoria, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia Goiano os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;

• Que cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia Goiano.

gov.br Documento assinado digitalmente
JOSE PEDRO ALVES NETO
Data: 04/06/2025 21:11:14-0300
Verifique em https://validar.iti.gov.br

CERES -GO
Local

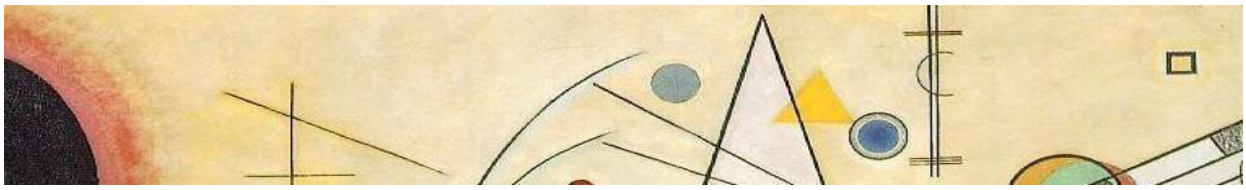
04 /06 /2025
Data

Assinatura do autor e/ou detentor dos direitos autorais

Ciente e de acordo:

gov.br Documento assinado digitalmente
ROITIER CAMPOS GONCALVES
Data: 09/06/2025 10:59:39-0300
Verifique em https://validar.iti.gov.br

Assinatura do(a) orientador(a)



Contemporânea
Contemporary Journal
Vol. 5 N°. 5: p. 01-12, 2025
ISSN: 2447-0961

Artigo

SEGURANÇA E VULNERABILIDADES EM REDES WI-FI E MÓVEIS: RISCOS E PROTEÇÃO DE DADOS EM TRANSAÇÕES BANCÁRIAS

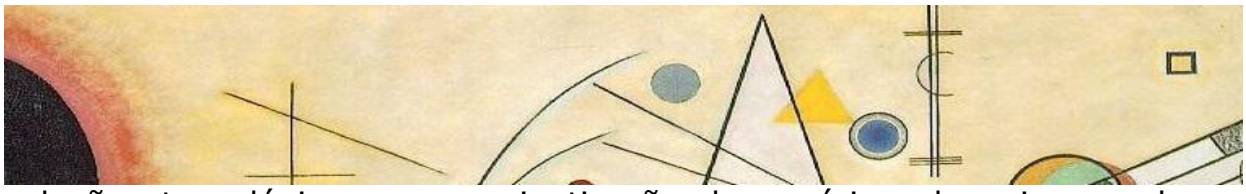
SECURITY AND VULNERABILITIES IN WI-FI AND MOBILE NETWORKS: RISKS AND DATA PROTECTION IN BANKING TRANSACTIONS

SEGURIDAD Y VULNERABILIDADES EN REDES WI-FI Y MÓVILES: RIESGOS Y PROTECCIÓN DE DATOS EN LAS TRANSACCIONES BANCARIAS

DOI: 10.56083/RCV5N5-126
Receipt of originals: 4/25/2025
Acceptance for publication: 5/16/2025

José Pedro Alves Neto
Graduando em Sistema da Informação
Instituição: Instituto Federal Goiano – campus Ceres
Endereço: Ceres, Goiás, Brasil
E-mail: jose.pedro@estudante.ifgoiano.edu.br

RESUMO: O crescimento do uso de redes Wi-Fi em dispositivos móveis tem facilitado o acesso a serviços digitais, incluindo transações bancárias, mas também aumentou a exposição a ciberameaças. Diante desse cenário, este artigo investiga as principais vulnerabilidades das redes Wi-Fi e seus impactos na segurança das transações financeiras realizadas por meio de smartphones. O objetivo é identificar os riscos mais recorrentes, analisar as fragilidades dos protocolos de segurança e propor medidas de mitigação. A metodologia utilizada envolve revisão bibliográfica de publicações recentes nas áreas de segurança da informação, redes sem fio e cibersegurança, com foco em estudos de caso e diretrizes técnicas. Os resultados apontam para a presença de ataques como Man-in-the-Middle, interceptação de pacotes e exploração de redes públicas inseguras, evidenciando a fragilidade de conexões desprotegidas. A pesquisa destaca ainda a eficácia de práticas como autenticação multifatorial, uso de VPNs e criptografia avançada na proteção de dados sensíveis. Conclui-se que, além da implementação de



soluções tecnológicas, a conscientização do usuário sobre riscos e boas práticas é fundamental para reduzir vulnerabilidades e garantir a segurança das informações durante transações bancárias em redes Wi-Fi.

PALAVRAS-CHAVE: segurança da informação, redes Wi-fi, transações bancárias, ataques cibernéticos, criptografia, VPN.

ABSTRACT: The growing use of Wi-Fi networks on mobile devices has facilitated access to digital services, including banking transactions, but it has also increased exposure to cyber threats. In this context, this article investigates the main vulnerabilities of Wi-Fi networks and their impact on the security of financial transactions carried out via smartphones. The objective is to identify the most common risks, analyze the weaknesses in security protocols, and propose mitigation measures. The methodology is based on a literature review of recent publications in the fields of information security, wireless networks, and cybersecurity, focusing on case studies and technical guidelines. The results reveal the occurrence of attacks such as Man-in-the-Middle, packet interception, and the exploitation of unsecured public networks, highlighting the fragility of unprotected connections. The research also emphasizes the effectiveness of practices such as multi-factor authentication, VPN use, and advanced encryption in protecting sensitive data. It is concluded that, in addition to implementing technological solutions, raising user awareness about risks and best practices is essential to reduce vulnerabilities and ensure the security of information during banking transactions over Wi-Fi networks.

KEYWORDS: information security, wi-fi networks, banking transactions, cyber attacks, encryption, multi-factor authentication, VPN, man-in-the-middle.

RESUMEN: El creciente uso de redes Wi-Fi en dispositivos móviles ha facilitado el acceso a servicios digitales, incluidas las transacciones bancarias, pero también ha incrementado la exposición a amenazas cibernéticas. En este contexto, el presente artículo investiga las principales vulnerabilidades de las redes Wi-Fi y su impacto en la seguridad de las transacciones financieras realizadas a través de teléfonos inteligentes. El objetivo es identificar los riesgos más frecuentes, analizar las debilidades en los protocolos de seguridad y proponer medidas de mitigación. La metodología se basa en una revisión bibliográfica de publicaciones recientes en las áreas de seguridad de la información, redes inalámbricas y ciberseguridad, enfocándose en estudios de caso y directrices técnicas. Los resultados revelan la presencia de ataques como Man-in-the-Middle, interceptación de paquetes y explotación de redes públicas no seguras, evidenciando la fragilidad de las conexiones desprotegidas. La investigación también destaca

la eficacia de prácticas como la autenticación multifactor, el uso de VPN y el cifrado avanzado en la protección de datos sensibles. Se concluye que, además de implementar soluciones tecnológicas, la concienciación del usuario sobre los riesgos y las buenas prácticas es fundamental para reducir las vulnerabilidades y garantizar la seguridad de la información durante las transacciones bancarias a través de redes Wi-Fi.

PALABRAS CLAVE: seguridad de la información, redes wi-fi, transacciones bancarias, ataques cibernéticos, cifrado, VPN.

1. Introdução

O crescimento do uso de redes Wi-Fi e redes móveis tem proporcionado maior conveniência e acessibilidade para usuários domésticos e corporativos, facilitando atividades como transações bancárias de maneira rápida e prática. No entanto, essa facilidade de conexão também tem introduzido desafios significativos de segurança, com as redes sem fio tornando-se alvos frequentes de ataques cibernéticos (SILVA; OLIVEIRA, 2021). A ausência de medidas adequadas de proteção pode expor dados sensíveis, como credenciais bancárias, tornando operações financeiras vulneráveis (SANTOS; LIMA, 2020).

Esse cenário se torna ainda mais relevante ao observarmos os dados da pesquisa TIC Domicílios 2024, que revelam que 85% dos lares urbanos brasileiros já possuem acesso à internet — um crescimento expressivo frente aos 13% registrados em 2005. Além disso, aproximadamente 60% dos usuários acessam a internet exclusivamente por meio de smartphones, número que chega a 86% entre as classes D e E, grupos que geralmente possuem menos recursos para investir em segurança digital. Ainda segundo o levantamento, apenas 22% dos brasileiros possuem uma conectividade

considerada significativa, e entre os mais vulneráveis esse índice despenca para 3%. A pesquisa também aponta que 16% dos domicílios conectados compartilham sua conexão com vizinhos, uma prática que pode comprometer ainda mais a segurança das redes utilizadas para transações financeiras (CETIC.br, 2024a; CETIC.br, 2022).

Entre as principais ameaças, destacam-se os ataques *Man-in-the-Middle*, o *sniffing* de pacotes e as redes falsas (*Evil Twin*), técnicas que podem interceptar ou manipular informações trafegadas nas redes. Esses ataques representam um risco crescente, especialmente quando usuários se conectam a redes públicas ou desprotegidas para acessar aplicativos bancários em seus dispositivos móveis (NIST, 2020; CERT.br, 2021).

Este trabalho visa aprofundar a análise das vulnerabilidades existentes em redes Wi-Fi e móveis, com foco nos riscos associados às transações financeiras. Além disso, será realizada uma investigação baseada em relatórios de empresas de cibersegurança e em casos divulgados na mídia, para identificar as instituições bancárias mais expostas a falhas ou ataques nos últimos anos. A pesquisa pretende apresentar um panorama comparativo dos riscos enfrentados pelos principais bancos digitais e tradicionais no Brasil.

Por fim, o estudo abordará práticas e soluções recomendadas para mitigar esses riscos, como o uso de criptografia avançada, autenticação multifatorial, Rede Virtual Privada, (VPN), entre outras medidas. A intenção é oferecer informações relevantes tanto para usuários comuns quanto para instituições financeiras, contribuindo para um ambiente digital mais seguro.

2. Referencial Teórico

Com o avanço da conectividade móvel e a popularização das redes Wi-Fi, cresce também a preocupação com a segurança das informações trafegadas nesses ambientes. Embora essas tecnologias proporcionem

mobilidade e acessibilidade, elas também expõem os usuários a riscos significativos, sobretudo em transações bancárias realizadas via dispositivos móveis.

2.1 Categorias Teóricas Fundamentais

Segundo Stallings (2019), a arquitetura das redes Wi-Fi, por utilizar o meio aéreo como canal de comunicação, é intrinsecamente mais vulnerável que as redes cabeadas, pois qualquer dispositivo no raio de alcance pode tentar interceptar o tráfego. Essas vulnerabilidades são agravadas pela utilização de redes públicas, que muitas vezes operam sem criptografia ou com protocolos obsoletos, como o WEP, tornando os dados suscetíveis a interceptações e manipulações.

Ataques como o Man-in-the-Middle (MitM) são favorecidos por essas fragilidades. Nesse tipo de ataque, o invasor intercepta a comunicação entre o usuário e o servidor, capturando informações como senhas e dados bancários. Kim e Solomon (2014) enfatizam que esse tipo de ameaça é potencializado em redes sem criptografia ou com protocolos ultrapassados. Complementando essas vulnerabilidades, as chamadas redes falsas (Evil Twin) representam riscos adicionais, ao simularem pontos de acesso legítimos com o intuito de enganar o usuário e obter credenciais sensíveis.

Outro aspecto teórico relevante é o papel dos protocolos de segurança. O WPA3, por exemplo, surge como resposta às limitações do WPA2, oferecendo criptografia individualizada e maior proteção contra-ataques de força bruta, conforme abordado por Krause e Ross (2020).

Adicionalmente, a educação digital e a conscientização do usuário são amplamente discutidas na literatura como mecanismos de prevenção. Muitos usuários desconhecem os riscos associados ao uso de redes Wi-Fi públicas e, por isso, deixam de adotar medidas básicas de segurança. A proteção eficiente depende não só de tecnologia, mas também da capacidade crítica

do usuário em identificar comportamentos suspeitos e redes não seguras.

Relatórios de segurança de fontes como a Kaspersky (2023) e IBM X-Force (2022) reforçam que cerca de 25% dos ataques a instituições financeiras se originam em redes abertas, destacando a importância de práticas como autenticação multifatorial, uso de VPNs e monitoramento contínuo.

2.2 Análise Crítica dos Estudos de Caso

Casos reais ajudam a materializar os riscos mencionados pela literatura. Em 2021, clientes do Santander relataram fraudes após se conectarem a redes Wi-Fi gratuitas em locais públicos. Investigou-se o uso de redes Evil Twin, que imitavam conexões legítimas, redirecionando os usuários a páginas falsas de login bancário.

De forma semelhante, usuários do Nubank relataram movimentações suspeitas em 2022 após acessarem o aplicativo da instituição via redes abertas. O padrão identificado foi o de ataque Man-in-the-Middle, com interceptação do tráfego durante a comunicação do app com os servidores bancários. O Nubank respondeu com reforço nas diretrizes de segurança, recomendando o uso de VPNs e autenticação multifator.

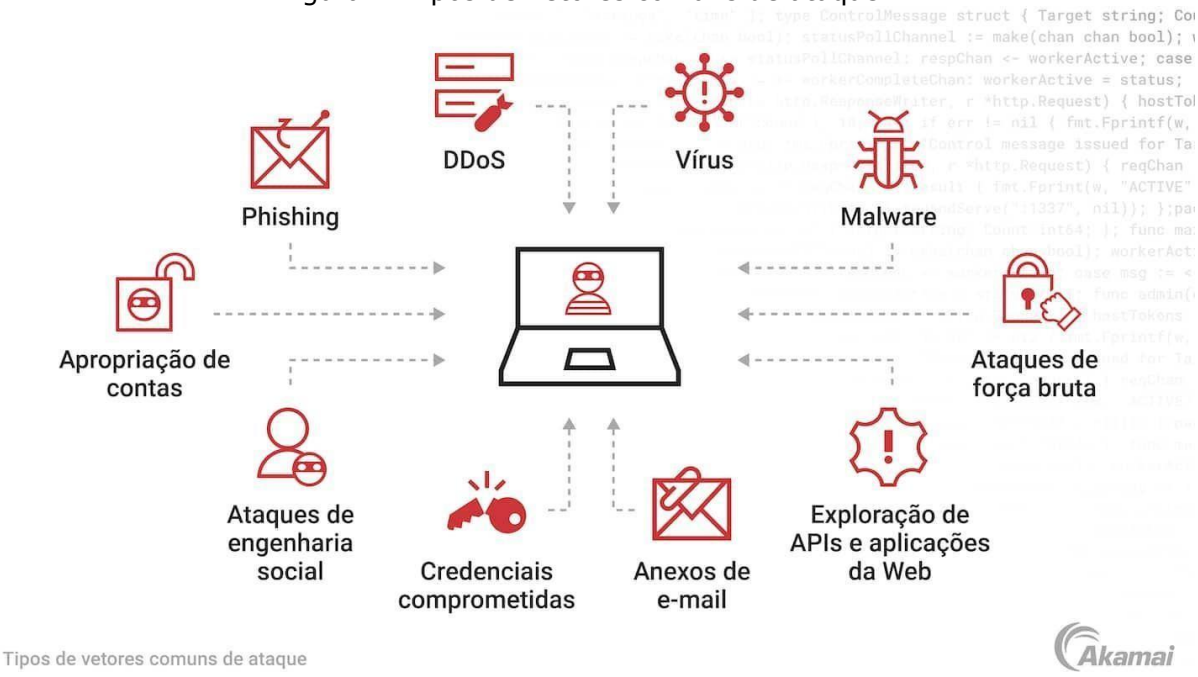
Embora o incidente do Banco Inter, em 2018, não tenha envolvido diretamente redes Wi-Fi, ele revelou fragilidades em APIs expostas, o que evidencia que a ausência de medidas robustas em qualquer ponto da cadeia de segurança digital pode favorecer ataques mais amplos, inclusive quando o usuário estiver conectado por Wi-Fi.

Esses exemplos reforçam que os riscos teóricos apontados por autores como Stallings (2019) e Kim e Solomon (2014) são concretizados na prática, especialmente quando usuários e instituições negligenciam protocolos e boas práticas de segurança.

2.3 Referência Visual Complementar

A Figura 1 resume os principais vetores de ataque cibernético que afetam a segurança digital, com destaque para phishing, malware, exploração de APIs e engenharia social técnicas comumente empregadas em ambientes com Wi-Fi desprotegido.

Figura 1. Tipos de vetores comuns de ataque.



Fonte: Akamai Technologies. *Tipos de vetores comuns de ataque*. Disponível em: https://www.akamai.com/pt/glossary/what-is-attack-vector. Acesso em: abr. 2025.

3. Metodologia

A presente pesquisa adota uma abordagem qualitativa e descritiva, com base em revisão bibliográfica e análise documental de casos reais de ataques cibernéticos envolvendo redes Wi-Fi. O levantamento teórico foi fundamentado em obras clássicas e atuais da área de segurança da informação, redes sem fio e proteção de dados, como Stallings (2019), Kim

e Solomon (2014) e Krause e Ross (2020), além de relatórios técnicos da Kaspersky, IBM X-Force e OWASP.

Para reforçar a conexão entre teoria e prática, foram incluídos estudos de caso amplamente divulgados na mídia e analisados por especialistas em cibersegurança. As fontes foram selecionadas com base na relevância, confiabilidade e atualidade, priorizando os anos de 2018 a 2023.

A pesquisa também considerou documentos oficiais de empresas de tecnologia e segurança digital (como Akamai e Psafe), permitindo a construção de um panorama realista e técnico sobre os riscos enfrentados por usuários e instituições financeiras no Brasil.

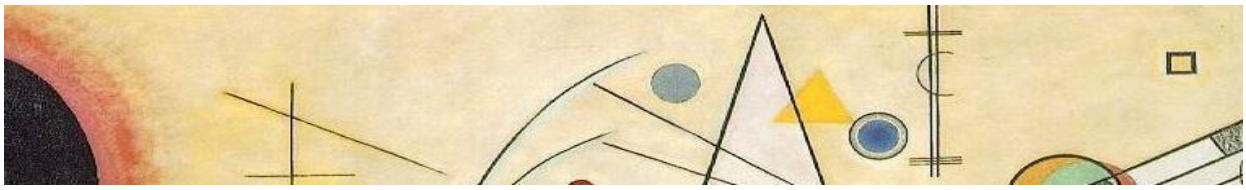
4. Resultados e Discussões

A análise dos dados coletados demonstrou que os ataques mais recorrentes em ambientes de Wi-Fi são o Man-in-the-Middle, a criação de redes falsas (Evil Twin) e a interceptação de pacotes (*packet sniffing*). Essas técnicas exploram falhas na configuração de redes abertas, uso de protocolos ultrapassados e comportamentos negligentes por parte dos usuários.

A implementação de medidas como VPNs, autenticação multifatorial e criptografia WPA3 mostra-se eficaz na mitigação dos riscos. Os dados da Kaspersky (2023) indicam que cerca de um quarto das tentativas de invasão em bancos ocorre por redes públicas sem segurança adequada.

Na discussão dos casos do Santander e Nubank, observou-se que, mesmo com medidas de proteção implementadas pelos bancos, a vulnerabilidade persiste quando o usuário ignora práticas básicas de segurança, como evitar redes públicas sem VPN ou autenticação adicional. Isso revela que a segurança da informação é um processo compartilhado entre instituição e consumidor.

Adicionalmente, os resultados revelam que bancos digitais, mais acessados por dispositivos móveis, apresentam maior exposição aos riscos



das redes Wi-Fi abertas, o que demanda investimentos constantes em educação do usuário e aprimoramento das infraestruturas de segurança.

5. Conclusão

Conclui-se que a utilização de redes Wi-Fi para transações bancárias, embora pratique e conveniente, ainda representa um vetor crítico de risco para a segurança da informação. A pesquisa demonstrou que as vulnerabilidades mais comuns estão associadas à ausência de criptografia, autenticação frágil e falta de conscientização dos usuários.

Medidas como autenticação multifatorial, uso de VPNs e protocolos como o WPA3 devem ser combinadas com ações educativas, promovendo uma cultura de cibersegurança tanto entre os usuários quanto nas instituições. Além disso, o monitoramento contínuo das ameaças e a realização de testes de segurança devem ser priorizados pelos bancos, principalmente os digitais.

O estudo reforça a necessidade de integração entre tecnologia, boas práticas e comportamento consciente, a fim de garantir maior resiliência às transações bancárias realizadas em redes Wi-Fi.

Agradecimentos

Expresso minha sincera gratidão ao professor Roitier Campos Gonçalves, orientador deste trabalho, pelo apoio, orientação técnica e incentivo constante ao longo de todas as etapas desta pesquisa. Sua experiência, disponibilidade e contribuições foram fundamentais para o aprofundamento do tema e para a consolidação deste artigo. Agradeço também ao Instituto Federal Goiano – Campus Ceres, pela estrutura acadêmica oferecida, pelo ambiente de aprendizagem propício ao desenvolvimento científico e pelo incentivo à produção de conhecimento. Este artigo foi desenvolvido durante

minha trajetória acadêmica no 7º período do curso de Bacharelado em Sistemas de Informação, e representa o esforço de consolidar os conhecimentos adquiridos ao longo da graduação.

Referências

AKAMAI TECHNOLOGIES. Tipos de vetores comuns de ataque. Disponível em: https://www.akamai.com/pt/glossary/what-is-attack-vector. Acesso em: abr. 2025.

CERT.br – CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de segurança para internet.** São Paulo: NIC.br, 2021. Disponível em: https://cartilha.cert.br. Acesso em: 5 ago. 2025.

CETIC.BR. **Em duas décadas, proporção de lares urbanos brasileiros com internet passou de 13% para 85%**, aponta TIC Domicílios 2024. São Paulo: Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação, 2024a. Disponível em: https://www.cetic.br/pt/noticia/em-duas-decadas-proporcao-de-lares-urbanos-brasileiros-com-internet-passou-de-13-para-85-aponta-tic-domicilios-2024/. Acesso em: 5 maio 2025.

CETIC.BR. **92 milhões de brasileiros acessam a internet apenas pelo telefone celular**, aponta TIC Domicílios 2022. São Paulo: Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação, 2022. Disponível em: https://www.cetic.br/pt/noticia/92-milhoes-de-brasileiros-acessam-a-internet-apenas-pelo-telefone-celular-aponta-tic-domicilios-2022/. Acesso em: 5 maio 2025.

IBM. **X-Force Threat Intelligence Index 2022.** IBM Security, 2022. Disponível em: https://www.ibm.com/reports/threat-intelligence. Acesso em: abr. 2025.

KASPERSKY. **Financial Cyberthreats 2023 Report.** 2023. Disponível em: https://securelist.com. Acesso em: abr. 2025.

KIM, David; SOLOMON, Michael G. **Fundamentos de segurança da informação.** 2. ed. Rio de Janeiro: Alta Books, 2014.

KRAUSE, James F.; ROSS, Keith W. **Redes de computadores e a internet: uma abordagem top-down.** 8. ed. São Paulo: Pearson, 2020.
NIST – NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Guidelines for securing wireless local area networks (WLANs)**. Gaithersburg: NIST, 2020.

SANTOS, André; LIMA, Karla. **Cibersegurança em redes Wi-Fi públicas: implicações para o setor bancário.** Anais do Congresso Nacional de Segurança da Informação, 2020.

SILVA, João; OLIVEIRA, Maria. **Segurança em redes sem fio: desafios e soluções atuais.** Revista Brasileira de Segurança Digital, v. 8, n. 2, p. 45–61, 2021.

STALLINGS, William. **Segurança em redes de computadores: princípios e práticas.** 6. ed. São Paulo: Pearson, 2019.